Security Quickie 36: Patches - More Fun Than A Barrel Of Monkeys

Sometimes it’s kind of hard to understand the significance of security vulnerabilities, or take the time to deal with them even when you do know how bad they can be. But it is important to patch systems and limit the threat from new vulnerabilities. For example, two recent Microsoft bulletins refer to a risk from a buffer overflow. In general, when something overflows, it can make a mess. In an information technology sense, a buffer overflow is where an attacker tries to stuff more data into a data structure than that structure can handle. This can result in almost no effect or, conversely, a huge, messy affair that can takes days to clean up after. Why the differences? Let me illustrate…

Let’s say that you have a big wicker monkey basket in your office that is has enough room to hold 4 monkeys. Let’s say that someone (either intentionally or accidentally) sends your basket 5 monkeys. Your receptionist does not know how many monkeys your basket can hold, so he just puts all the monkeys in the basket. Well, there is 1 monkey too many, and that extra monkey is free to get out and wonder around your office. Sometimes this extra monkey will just lay down and take a nap (nothing bad happens) and sometimes this extra monkey plays with your phone, turns the lights on and off, throws paper files around, pulls your hair, and generally makes it impossible for you to do your job (causing your system to crash).

Let’s say that Dr. Evil (the bad guy) knows that you have a monkey basket (an application) that holds only 4 monkeys. Dr. Evil also knows that your receptionist will put all the monkeys he sends you in the basket, even if he sends too many monkeys. Let’s also say that Dr. Evil wants to do bad things to you. He specially trains the monkey that will overflow the basket to perform dastardly acts. When he sends you 5 monkeys, he knows that there will be 1 monkey free to wonder around your office (your operating system) to do his bidding. Dr. Evil could train a monkey to call him on the phone so he could direct the monkey to do his bidding (this is called creating a shell). From here, Dr. Evil can do whatever he wants to do because the monkey can access anything inside the office.

Let’s say that the manufacturer of the monkey basket sends out an advisory (this is the vulnerability bulletin we receive) stating that the basket can only hold 4 monkeys, and that whoever puts the monkeys in the basket needs to count and allow only 4 monkeys in, and sends the 5th monkey in search of the man with the yellow hat. Now the receptionist knows how to handle incoming monkeys (the patch is applied) and won't be fooled into overflowing the basket.

That is in essence a buffer overflow. Sometimes a buffer overflow is accidental; sometimes it's intentional. Sometimes nothing bad happens, and sometimes Dr. Evil takes over your office. That's why it is important to apply patches that fix vulnerabilities, like buffer overflows. In a very real sense, patching really *is* more fun than a barrel of monkeys…